AIR WAR COLLEGE

AIR UNIVERSITY

SPYING FOR THE RIGHT REASONS:

CONTESTED NORMS IN

CYBERSPACE

by

Andreas Wachowitz, Lt Col (GS), German Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Paul J. Springer

6 April 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lt Col (GS), German AF, Andreas Wachowitz is assigned to the Air War College, Air University, Maxwell AFB, AL. He earned his pilot wings from ENJJPT in 1994 and held flying assignments as an instructor pilot, Flying Training Squadron executive officer in Holloman AFB, NM, and Squadron Commander of the 1st Squadron Tactical Reconnaissance Wing 51 "Immelmann" in Germany. He accumulated a total of over 2500 flying hours, of which over 2000 were flown in the Tornado and served on the Tornado Reconnaissance Wing during ISAF. He graduated from the General/Admiral Staff Officer Course in Hamburg in 2009. In the following assignments, he worked as a desk officer in the German Air Force Command, the Federal Ministry of Defense, and as a Section Chief in the Strategic Reconnaissance Command. On his last position, he was responsible for military intelligence doctrine and contributed to the organizational built up of the German Cyber Command.

Abstract

When former National Security Agency contractor Edward Snowden revealed that the United States was tapping the phone of German Chancellor Angela Merkel, he triggered an entirely new debate upon the changing international norms of espionage in the twenty-first century, especially the question of spying among allies. Additionally, taking advantage of cyber vulnerabilities might be perceived as a precursor to attack, and advanced persistence threats allow the exploitation of huge amounts of data, including intellectual property, on an unprecedented scale.

However, international norms have always been contested from a legal or ethical perspective and are not new in cyberspace. The reasons for deviating from norms in cyberspace will not be found in this specific domain but within the overarching context of international relations. Nations should not refrain from cyber-espionage in general just because the access to a system could be perceived as a precursor to attack, and spying on critical infrastructure in particular if the overall behavior of a potential adversary is sending a threatening message and state's survival might be at stake. Also, while it is obvious that economically motivated cyber-espionage is outside the norm, it is also alluring to cross this norm because cyber-espionage is a low risk and high payoff enterprise. Therefore, limits have to be articulated and agreed upon and the international community has to interweave these agreements in other mechanisms outside the virtual world to underpin their value. And lastly, even allies should be aware that there is no such thing as unconditional trust. Nevertheless, it is of utmost importance that states adhere to more restraining norms when "verifying" on allies in lieu to spying on adversaries to avoid damage to the unity of alliances and common values.

Introduction

In June 2013, former National Security Agency (NSA) contractor Edward Snowden revealed that the United States was spying on 122 political leaders around the world. Surprisingly, even though Germany is known as one of the closest allies to the United States German Chancellor Angela Merkel was among those leaders. The list showed more than 300 automated intercepted conversations.[1] In addition to shocking the world with the NSA's technological prowess, Snowden's leak triggered an entirely new debate upon the changing international norms of espionage in the twenty-first century. Cyber capabilities have enabled the quiet extraction, from a safe distance, of unprecedented volumes of data. Also, once a state has exploited the vulnerabilities of a system to get access, it can easily change its intent from espionage to sabotage or even attack. These possibilities raise the question: what are the norms governing cyber-espionage, particularly among closely allied states? And do those norms need revision in light of the new capabilities?

Legal Considerations and Assumptions

It seems that there is an obvious paradox in defining norms for espionage. On the one hand, states are involved in spying activities in many other countries while on the other hand, they ban espionage within their own territory by domestic law.[2] Moreover, it appears that international law avoids directly addressing the topic of espionage. Therefore, it is necessary to look for other indications that might work as a guideline for state's behavior in this realm.

---

1 "Snowden Archive," CJFE | Canadian Journalists for Free Expression, accessed December 16, 2016, http://www.cjfe.org/snowden; "GCHQ and NSA Targeted Private German Companies - SPIEGEL ONLINE," accessed December 16, 2016, http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

2 William A. Owens et al., eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, DC: National Academies Press, 2009), 259.

A. John Radsan describes espionage as a subset of covert action and cites the U.S. National Security Act of 1947 that further explains that those actions are directed to change other nation's behavior or alter their capabilities in a way that U.S. involvement can be denied.[3] Thomas Rid basically asserts the same for the cyber domain and defines this type of covert action a cyber-attack. He further claims that "[a]ll politically motivated cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion."[4] Within these contexts, international law and international customary law offer an approach to constraining states' activities in espionage. First, Article 2(3) of the United Nations (UN) Charter indicates that states should solve their issues by peaceful means and second, paragraph (4) says that they should honor the territorial integrity and political independence of any state and therefore refrain from the threat or use of force. The third threshold within the UN Charter is the state's right of self-defense (Article 51), anticipatory (or pre-emptive), in the case of an armed attack by another state.[5] It is noteworthy to point out that there is a distinction between "use of force" in the former Article and "armed attack" in the latter one since not all unlawful use of force rises to the level of an armed attack. In short, the first norm that can be concluded from international law is that espionage should not interfere in another country's

3 A. John Radsan, "The Unresolved Equation of Espionage and International Law," *Michigan Journal of International Law* 28, no. 3 (2007): 599.

4 Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 1 (February 2012): 5.

5 UN Charter Article 2(3): "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."
UN Charter Article 2(4): "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."
UN Carter Article 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

sovereignty and should not cross the threshold of unlawful use of force unless the findings warrant the purpose of self-defense or anticipatory self-defense. It is beyond the scope of this paper to prove that international law is applicable to cyberspace or that cyber-attacks can indeed reach the level of force or armed attack. However, Walter Sharp's *Cyberspace and the Use of Force* and the *Tallinn Manual* discuss this issue at length and conclude that both are applicable to cyberspace.[6]

Understanding international law is difficult because it is based upon a different philosophy than domestic law. Domestic laws in Western democracies are very deliberate and precisely articulated to protect individuals from the state's power and to avoid arbitrary judgments and punishments when a certain law is violated. In contrast, the principle of international law is to honor the state's sovereignty and set some boundaries of self-imposed norms in international relations. Therefore, the wording used is very broad, and an interpretation of these norms varies by perception and can only be derived in studying states' practices.[7] Cyber technology, even though it has expanded and evolved very rapidly, in these terms is still in its infancy, which makes it difficult to study states' practices.

It seems that the developments in cyber technology are outpacing international norms as developed states become more and more dependent on cyber technology. On the one hand, they improve their prowess in this field, including the capability to inflict cyber harm, but on the other hand, they also become more vulnerable to cyber-attacks.[8] However, "the distinction between a

6 Walter Gary Sharp, *Cyberspace and the Use of Force* (Falls Church, Va: Aegis Research Corp, 1999); Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, eds., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge ; New York: Cambridge University Press, 2013).

7 Ian Hurd, "The International Rule of Law: Law and the Limits of Politics," *Ethics and International Affairs* 28, no. 1 (2014): 39–51.

8 Richard A. Clarke and Robert K. Knake, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed (New York: Ecco, 2010), 44–47.

cyberattack and a cyberexploitation may be very hard to draw from … since both start with taking advantage of a vulnerability."[9] The second problem in cyber-espionage is the fact that a large amount of information can be extracted over just a short period of time, including data of intellectual property (IP). A distinction between espionage for security reasons and economically motivated cyber-espionage (EMCE) is hardly possible anymore.[10] Lastly, cyber-espionage has a low cost, high payoff, and is difficult to detect.[11] This makes it alluring for governments to eavesdrop not only on their adversaries but also on their friends, and it appears that the disclosure of the Snowden documents confirms this allegation.[12] It is the purpose of this paper to discuss the three sub-contexts of cyber-espionage—the ambiguity of taking advantage of cyber vulnerabilities, EMCE, and spying on friends—within the ethical and legal framework and to conclude appropriate norms from this discussion.

9 Owens et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 261.

10 Martin C. Libicki, *Cyberspace in Peace and War* (Annapolis, Maryland: Naval Institute Press, 2016), 342.

11 Clarke and Knake, *Cyber War*, 232.

12 Leif-Eric Easley, "Spying on Allies," *Survival* 56, no. 4 (September 2014): 142.

Thesis

The requirement for states to conduct espionage is based on their perception of threat. Espionage can range from the verification of positive attitudes towards one another to the confirmation of a hostile or criminal intent of another country. This knowledge is mandatory to prepare diplomatic and/or military responses which seem to be necessary for a state's survival or mutual trust. Cyber-espionage is just another tool to conduct espionage, which makes it easier but not different from the traditional method. Therefore, universal norms cannot be deduced from an isolated discussion of behavior in cyberspace, but have to be viewed within the overarching context of each case. Moreover, the threat to a state's survival will always supercede given norms and countries are likely to cross the limits if thereby open hostilities can be avoided. Nevertheless, states should articulate their thresholds within cyberspace to communicate what they perceive as a threat and to ensure the international community is aware that a violation of these thresholds will not be tolerated.

Espionage

The common literature on espionage deals mainly with the study of historical cases and how it contributed to or spoiled a military operation. In the context of international law, most scholars discuss espionage from the *Jus in Bello* perspective that is from the background of the Geneva Convention or The Hague Regulations.[13] One focus is the distinction between military intelligence and espionage. Usually, military intelligence collection involves activities that do not violate any law, either domestic or international. For example, an aircraft flying along an international border that triggers the other country's air defense radar with the intend to record the emission for the exploitation of the radar signature is considered legal.[14] Moreover, "military intelligence" is even accepted within *Jus in Bello*. A military reconnaissance team that operates behind enemy lines in an overt mission and wearing a uniform or other identifying artefacts in accordance with the Geneva Convention is therefore protected by international law, if captured, and has to be treated as prisoners of war rather than an individual engaged in espionage.[15] However, Radsan points out that there is a lack of literature dealing with espionage during peacetime. Those scholars that discuss this issue represent three factions; those that claim that espionage is legal, those who say it is not, and those who suggest that the answer depends upon context.[16]

Espionage is Legal, if…

International law neither allows espionage nor explicitly prohibits it. Therefore, there is an ongoing discussion whether it should be considered legal or illegal. Especially, the discussion

13 Radsan, "The Unresolved Equation of Espionage and International Law," 601.

14 Owens et al., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 261.

15 Radsan, "The Unresolved Equation of Espionage and International Law," 601–2.

16 Ibid., 602.

on espionage during peacetime is divided among scholars. According to Radsan, a reason why some authors consider spying illegal under international law is the argument that it violates the territorial integrity and political independence of another state.[17] This argument, however, fails to recognize that Article 2 (4) of the UN Charter just prohibits the "threat or use of force" to interfere with the territorial integrity and political independence and not espionage per se.[18] Many authors, however, argue that espionage is legitimate because it is part of a state's right of anticipatory self-defense.[19] Sharp even underpins this argument and ties it to the 1961 Vienna Convention that "…explicitly recognizes the well-established right of nations to engage in espionage during peacetime and […] clandestine intelligence collection activities as an inherent part of foreign relations and policy."[20] State practice also suggests that espionage is accepted internationally since no international treaty explicitly prohibits or restricts states' involvement. Hays Parks brings it to the point when he says that "[n]o serious proposal has ever been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgment by nations that it is important to all, and practiced by each."[21]

For the purpose of this essay, it is important to address the nexus between (anticipatory) self-defense and espionage. According to Article 51 of the UN Charter, a state has the right to act in self-defense in response to an armed attack, or according to customary law, to act pre-emptively if such an attack is imminent.[22] The military capabilities of a country by itself do not

17 Ibid., 604–5.

18 "Charter of the United Nations | United Nations," accessed November 28, 2016, http://www.un.org/en/charter-united-nations/index.html.

19 Radsan, "The Unresolved Equation of Espionage and International Law," 603–4.

20 Sharp, *Cyberspace and the Use of Force*, 123.

21 W. Hays Parks, "The International Law of Intelligence Collection," in National Security Law, ed. John Norton Moore, Frederick S. Tipson, and Robert F. Turner (Durham, N.C: Carolina Academic Press, 1990), 433–34.

22 "Charter of the United Nations | United Nations."; Owens et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 243.

warrant a pre-emptive reaction. However, if a state's overall behavior indicates aggression against the other state, and if this aggression is now further aggravated by troop deployments along the border, anticipatory self-defense might be a legitimate response. In other words, risks become a threat if they are accompanied by hostile intent. Unless there is an open declaration of war, the only way to find out the real intent of a country is by espionage. The NATO Intelligence Warning system continuously monitors activities in the world. As soon as the behavior of a region or country indicates the approach of a crisis, further intelligence gathering, including espionage by member states' agencies, is guided in that direction for the purpose to determine whether the behavior of that country might become a threat.[23] On the same token, espionage might also prove the opposite, the lack of hostile intent or simply serve as a means to verify that states act as they say. That way espionage kills two birds with one stone; it contributes to peaceful international relations and protects nations from a hostile intent.[24] In summary, this essay is based on the assumption that espionage is legitimate in legal and moral terms as long as it serves the purpose to verify or deny possible threats and remains below the threshold of threat or use of force of Article 2 (4) of the UN Charter. The question is, what do these findings mean in the virtual realm?

Espionage in Cyberspace

First of all, there is also the distinction between intelligence gathering and espionage in cyberspace. The interception of openly transmitted data within networks is the same as intercepting radio signals during traditional military intelligence. Cyber is just a new medium to communicate and as long as there is no forceful intrusion into a system it remains in the domain

23 "Nato Review," accessed December 4, 2016, http://www.nato.int/docu/review/2002/issue4/english/art4.html.

24 Parks, "The International Law of Intelligence Collection," 433.

of legally uncontested intelligence collection.[25] Also, it is noteworthy, that any exploitation of a vulnerability in cyberspace is considered an attack, however, cyber-espionage should not be confused with an attack from a military viewpoint. To avoid misinterpretation, the U.S. Department of Defense Law Manual separates the cyber-attack from the meaning of an attack in a military sense.[26] From the perspective of international law, cyber-espionage is only legitimate for the same reasons as traditional espionage, which means that states should only utilize cyber-tools if they can ensure that they do not cross the threshold of threat or use of force. The *Tallinn Manual*, as well as Sharp, acknowledge that the means available in cyberspace can certainly cross this threshold. The *Tallinn Manual* asserts that inter alia manipulating news or the shutdown of a party's information campaign already interferes with the non-intervention rule of the UN Charter and considers it as "use of force."[27] Sharp further explains that cyber operations are able "… to even cause physical destruction from remote locations abroad."[28] However, the problem in cyberspace is the ambiguity of code, content, and intent, and the difficulty in attribution. To further explain these difficulties, it is necessary to elaborate upon cyber-espionage.

25 Clarke and Knake, *Cyber War*, 37.

26 Office of General Counsil Department of Defense, "Department of Defense Law Manual," June 2015, 987. 16.1.3.2 Cyber Attacks or Computer Network Attacks. The term "attack" often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services. Operations described as "cyber attacks" or "computer network attacks," therefore, are not necessarily "attacks" for the purposes of applying rules on conducting attacks during the conduct of hostilities. Similarly, operations described as "cyber attacks" or "computer network attacks" are not necessarily "armed attacks" for the purposes of triggering a State's inherent right of self-defense under jus ad bellum.

27 Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 42–45.

28 Sharp, *Cyberspace and the Use of Force*, 19.

Cyberspace and Espionage

In the common literature, hardly any book deals explicitly with cyber-espionage itself. Scholars usually discuss this topic among the broader concept of cyber warfare or approach it in separate articles. None of the literature that was reviewed for this essay contested the legitimacy of cyber-espionage. The authors mainly focus on the ambiguity of the code that is used and how it can be misinterpreted as an attack, thus igniting or escalating a conflict. Richard Clarke states that there is only a small step between spying and causing damage to diplomacy because the code used to get access to a system might be misinterpreted for the "preparation of the battlefield."[29] Libicki broadens the discussion and raises the question of whether not only the code itself but also the quantity which can easily be extracted by cyber-espionage, justifies the *Jus ad Bellum.*[30] However, all authors agree that "[t]he technology of computers and the internet allows a lawful act of espionage to materialize into an unlawful use of force at the speed of light."[31] The ethical aspect of cyber-espionage concentrates heavily on EMCE. The authors agree that EMCE cannot be justified as "espionage" and consider it a criminal act and simultaneously acknowledge that nations lack the mechanisms to separate security motivated espionage from EMCE.[32] It appears that the moral aspects of spying among allies are hardly researched at all. Leif-Eric Easley examined the factor of trust in the context of international relations. He concludes that even though trust is important there is also the need to verify.[33] It appears that available tools in cyberspace have opened Pandora's Box and that all the problems are unique to the cyber domain. Moreover, many authors try to find a panacea within cyberspace

29 Clarke and Knake, *Cyber War*, 228–37.
30 Libicki, *Cyberspace in Peace and War*, 324.
31 Sharp, *Cyberspace and the Use of Force*, 129.
32 Libicki, *Cyberspace in Peace and War*, 342.
33 Leif-Eric Easley, "Spying on Allies."

or at least try to contain the problems there to avoid an escalation into the physical world. But both assumptions are flawed. Neither are the problems unique in cyber nor will we find the solutions there.

Espionage or Attack?

Espionage for the purpose of self-defense is tolerated under international law as long as the state refrains from the threat or use of force as stated in the UN Charter. One argument against cyber-espionage is the ambiguity of intent when taking advantage of the vulnerability of a system. Imagine that someone gains access to the router of someone's home network. Once inside the administration set up, the perpetrator could just retrieve the data from the device, for example, how many clients are connected to the network; or start to manipulate the router's settings; or print a few pages of Guy Fawkes masks just to annoy the owner. The vulnerability used to get access to exploit information is the same that can be used to launch an attack. Aron Brantly states in his essay that "[a] given malware or malicious behavior resulting in cyber espionage (CE), offensive cyber operations, or defensive cyber operations-response action (DCO-RA) is often indistinguishable absent context or significant forensic analysis."[34] The same principle applies at the state level but with more serious impacts since evolved nations become more and more cyber-dependent. Today, networks host many of U.S. critical infrastructures like transportation systems or electrical nodes.[35] On the one hand, if the code is used for cyber-espionage, the use would be within the legal means of a country. If on the other hand the same code is used for the purpose of sabotage, as Thomas Rid frames the intent to deliberately destroy or weaken an economic or military system, it would certainly cross the level

34 Aaron F. Brantly, "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace," *Intelligence and National Security* 31, no. 5 (July 28, 2016): 675.

35 Clarke and Knake, *Cyber War*, 226–27.

of unlawful use of force as defined by Sharp or the *Tallinn Manual*.[36] Does that mean that states should ban all cyber-espionage to avoid crossing the use of force threshold, or at least restrain themselves from spying on critical infrastructure? There are two reasons why they should not. First, the ambiguity between espionage and sabotage is not unique in cyberspace and has always been part of a state's portfolio to influence other nations. As pointed out, espionage is a subset of covert action and by the defined legal assumption the only legitimate form of covert operations. However, the U.S. Central Intelligence Agency (CIA) conducts all types of covert missions, which means that a spy may turn into a saboteur in the nick of time. That makes basically every spy as ambiguous as the malicious code used for cyber-espionage.[37] Especially, if the acquired information reveals an imminent threat to the country, the nation might task the same agency and maybe even the same individual to mitigate the risk, despite the fact that this covert act of sabotage will most probably violate international law. But also from a technological perspective, these ambiguities have always been present. The United States exploited the Soviet Union's inability to protect its airspace at high altitude and conducted U-2 reconnaissance flights over Soviet territory. These airplanes could have been easily equipped with a weapon. The Soviets claimed that they felt threatened and ultimately shot one of these spy planes down when they were finally capable, putting an end to the missions.[38] In the future, the capabilities of the F-35 could also allow stealthy intelligence missions by the exploitation of the vulnerabilities of today's air defense systems but since the Joint Strike Fighter is also a weapon platform, the intent would be more ambiguous.[39]

36 Thomas Rid, "Cyber War Will Not Take Place," 16.

37 Owens et al., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 261.

38 Sharp, Cyberspace and the Use of Force, 120–27.

39 "F-35 Capabilities," F-35 Lightning II, accessed December 18, 2016, https://www.f35.com/about/capabilities.

Exacerbating the ambiguity problem is the fact that states actually use covert missions, sometimes on a large scale, to interfere in another nation's sovereignty. The CIA sabotaged Cuban economics in the late 1950s and even tried to overthrow Castro's regime with a futile attempt to invade the country in 1961 at the Bay of Pigs.[40] Also in 1953, the CIA had inspired a coup in Iran to overthrow the government and replace the old leader with one favorably disposed toward the U.S.[41] However, with the mindset of the Cold War and the perceived threat emanating from these countries, the United States did what they believed was in the interest of the state's survival and even though they violated international law they still avoided the outbreak of a war.

Espionage on critical infrastructure might be warranted by the circumstantial behavior of a state. Libicki explains that the Geneva Conventions prohibits deliberate deception. For example, states must not disguise combatants as non-combatants or exploit schools and hospitals as command and operation centers.[42] A violation of this principle in cyberspace could mean that nations are hiding their military activities behind civilian enterprises which might warrant espionage on those critical infrastructures. A good example to illustrate this behavior is the effort of states to gain access to nuclear weapons which they often hide behind proclaimed peaceful power programs. In the 1970s, Iraq pursued a nuclear agenda and pretended it was necessary to secure electricity for the country. Israel monitored these activities closely and decided to destroy the reactor in 1981 when they found out that Iraq rejected the use of uranium for this facility and tried to acquire plutonium instead.[43] Similar to this incident, Israel attacked a

40 David Patrick Houghton, *The Decision Point: Six Cases in U.S. Foreign Policy Decision Making* (New York: Oxford University Press, 2013), 88–91.

41 Ibid., 167.

42 Libicki, *Cyberspace in Peace and War*, 321.

43 "Operation Opera - Raid on Iraqi Nuclear Reactor | Jewish Virtual Library," accessed November 15, 2016, http://www.jewishvirtuallibrary.org/jsource/History/Osirak.html.

nuclear enrichment facility in Syria in 2007 because of the fear of the proliferation of Weapons of Mass Destruction (WMD) to a regime that had already threatened Tel Aviv with annihilation.[44] In 2010, Stuxnet was discovered. This highly sophisticated attack code, based on a whole of government effort toward espionage, intentionally targeted the critical infrastructure of a sovereign nation. It physically destroyed centrifuges in Iran's nuclear facility, where Teheran allegedly enriched uranium to weapons-grade purity. This attack proved that states are capable of conducting covert physical destruction by means of cyber-tools.[45]

The bottom line is that nations cannot restrain themselves from cyber-espionage in general just because the access to a system could also be a precursor to attack, and spying on critical infrastructure in particular if the overall behavior of a perceived adversary is sending a threatening message and state's survival might be at stake. But not only the ambiguity of code seems to be a problem in cyberspace. The ambiguity of the content of the stolen material is also challenging, especially if the extracted information contains both security and economic data.

State Survival or Economic Boost on the Cheap?

Many civilian business companies do not defend themselves sufficiently against cyber-threats in general, and cyber-espionage in particular. So, it is fairly easy for activists or criminals to steal confidential information. But even companies with high-level cyber security appear helpless when confronted with the capabilities at the disposal of a government. It is nearly impossible to prevent a state-sponsored attack and it is very difficult to prove the intent that it was conducted for economic benefit. Therefore, a solution to mitigate EMCE has to be found or at least supported by means outside cyberspace.

44 Jewish Policy Center, "The Attack on Syria's Al-Kibar Nuclear Facility," *Jewish Policy Center*, February 28, 2009, https://www.jewishpolicycenter.org/2009/02/28/the-attack-on-syrias-al-kibar-nuclear-facility/.

45 Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 212–32.

A code that opens a back door into a system is hard to detect, and thus might serve the intruder for years. Advanced Persistent Threat (APT) is the name that goes along with this kind of intrusion into a protected network. Many attacked companies only learn about the cyber-theft when the Federal Bureau of Investigation (FBI) informs them about it.[46] Paul Rosenzweig points out that EMCE is not only hurting business companies but also the state in its pursuit of growth and prosperity, and blames China for most of the damage.[47] The Director of National Intelligence confirms this claim and states that China has stolen intellectual property (IP) at a large scale for own economic advantages.[48] And Libicki illustrates that the Chinese are not even seriously hiding their trails during their criminal endeavors, however, that by itself does not prove a state's involvement.[49] Nevertheless, after the Snowden disclosures, even the United States had to admit that they also committed economic espionage, although Washington repudiated the accusation that it was for economic gain.[50] This illustrates the problem in this discussion. When is cyber-espionage against industrial companies justified for security reasons, and when is it outlawed as a criminal activity? Exacerbating the situation is the fact that the physics of cyberspace enable APTs to steal information in an amount which was not possible before the information age, which makes it a high payoff activity for states. From 2007 until 2009, someone hacked into the network of Lockheed Martin and stole a tremendous amount of IP related to the F-35's program. While the exact volume of the stolen data is not known for certain, the German magazine *Der Spiegel* claims that it amounts to many terabytes. Even just

46 Libicki, *Cyberspace in Peace and War*, 9–11.

47 Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, The Changing Face of War (Santa Barbara, Calif: Praeger, 2013), 94–95.

48 J. R. Clapper, "Statement for the Record, 'Worldwide Threat Assessment of the US Intelligence Community' before the House Permanent Select Committee on Intelligence," ed. DNI, February 25, 2016, 3.

49 Libicki, *Cyberspace in Peace and War*, 9–11.

50 Ibid., 255.

one terabyte equals "…ten copies of the *Encyclopedia Britannica*, all 32 volumes and 44 million words, ten times over."[51] While the intrusion into Lockheed Martin's servers actually resembles espionage, the amount of data stolen makes it nearly impossible to differentiate between economic and defense information because the company also has civilian programs in its portfolio. In these cases, it is hard to prove the intent of the attacker, especially since it takes years before IP theft is actually turned into a product.[52] Another reason why it is so attractive to conduct EMCE is the low risk associated with it. In traditional espionage, the spy used to risk his life when he tried to steal secrets from a country, and additionally, the receiving nation had the risk that the spy was a double agent who provided falsified data. Cyberspace eliminates both risks simultaneously since it is not necessary to enter the target state anymore and the likeliness to hit a purposely falsified database is very remote.[53] With so many advantages, no state really wants to abolish cyber-espionage, but they also recognize the threat to economic growth and prosperity. The UN Group of Government Experts (UN GGE) for Internet and Communication Technologies (ICTs), among them all leading cyber nations like the U.S., China, and Russia, agreed not to ban cyber espionage but on the same token proclaim that nations should restrict themselves to espionage purely for security reasons.[54] President Obama and Chinas President Xi underpinned this agreement during bilateral talks in September 2015 and confirmed their intention to refrain from EMCE. However, both statements still remain diffuse since security is a broad term and Washington and Peking also agreed that even "…commercial cyber-espionage

51 "Cyber-Attacke: Hacker Knacken Geheimes Jet-Projekt - SPIEGEL ONLINE," accessed December 17, 2016, http://www.spiegel.de/netzwelt/tech/cyber-attacke-hacker-knacken-geheimes-jet-projekt-a-620208.html; Clarke and Knake, Cyber War, 234.

52 Libicki, *Cyberspace in Peace and War*, 255.

53 Clarke and Knake, *Cyber War*, 234–35.

54 "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," *CCDCOE*, August 31, 2015, https://www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.

is allowed as long as the results are not given to commercial firms."[55] While the agreements are a good start into the right direction it is important to underpin them with measures in the physical world since there are no effective monitoring mechanisms in cyberspace yet.[56] Even though it is obvious that EMCE is outside mutually agreed norms the associated low risk and high payoff makes it alluring to conduct it. But cyber-espionage is not only appealing for EMCE, it is also tempting states to cross other ethical boundaries. One of these boundaries is the question of trust among allies.

Do Nations have Friends?

Tapping phone calls by a keystroke and effortlessly reading personal emails makes cyber-espionage really hard to resist. But should friends or allies really do this to each other? It even appears to be contradictory that on the one hand, nations collaborate in an intelligence cooperation and share secret information from various sources, while on the other hand, they tap the phones of each other's political leaders. However, actually it is not and it even makes sense if nations abolish their offended pride and think about it in a different way.

After Snowden revealed the spying activities of the NSA upon many political leaders who had called themselves friends of the United States there was an outcry across the world that espionage upon friends is unacceptable, and that this constitutes a serious breach of trust. Among those leaders was Germany's Chancellor Angela Merkel, who stated that both nations now have to find a way to reestablish this trust.[57] Although the NSA Affäre (NSA Affair) is still under investigation in Germany, the rhetoric has subsided, and President Obama received a very

55 Libicki, *Cyberspace in Peace and War*, 344–45.
56 Ibid., 345.
57 Leif-Eric Easley, "Spying on Allies," 142.

warm welcome on his farewell visit to Berlin.[58] The answer why the relationship returned to business as normal in such a short time is fairly easy; there are no friends among states. Colin Dueck points out that from a realist's perspective, the grand strategy of a nation only serves its own interests.[59] Additionally, Easley explains that there cannot be an unconditional trust among nations because in every nation, especially democracies, politics depend on domestic interests and national parties. The domestic political translation into international relations may change after an election or from internal pressure, thus providing a reason for the surveillance of the internal development. He further states that this "breach of trust," if revealed, should not be confused with "political betrayal."[60] The recent history of Germany illustrates the importance of surveillance of a political regime in order to verify that the politics do not hide bad intentions. When the Federal Republic of Germany was founded in 1948, it was in the interest of the Allies to monitor German leadership closely which could easily be done due to the occupying status of the Allies. Even though the United States chose the first Chancellor, Konrad Adenauer, it was not clear how long he could stay in power and whether his successor would revert back to nationalist policies.[61] A few years later, Germany demanded the rearmament of the country to counter the threat emanating from the Soviet Union.[62] In that regard, it is hard to believe that the allies did not verify their trust in the new country, especially because the USSR offered a reunification of Germany in return for its guaranteed neutrality.[63] And when the Iron Curtain (and with it the Berlin Wall) came down in 1989, Margaret Thatcher still distrusted Chancellor

58 Zweites Deutsches Fernsehen (ZDF), "US-Präsident in Berlin: Merkel Und Obama Werben Für TTIP - Heute-Nachrichten," accessed December 9, 2016, http://www.heute.de/treffen-im-kanzleramt-merkel-empfaengt-obama-und-wird-vom-us-praesidenten-gelobt-45923046.html.

59 Colin Dueck, *Reluctant Crusaders: Power.* (Princeton University Press, 2008), 11.

60 Leif-Eric Easley, "Spying on Allies," 142–43.

61 Joseph Shattan, *Architects of Victory: Six Heroes of the Cold War* (Washington, DC: Heritage Foundation, 1999), 103–7.

62 Ibid., 114–18.

63 Ibid., 123–28.

Helmut Kohl and tried to persuade France of a "German threat" which needed a counterbalance.[64] From the end of WWII until the end of the Cold War and beyond, it was always in the interest of the United States and its allies to verify German politics despite their growing "friendship" and mutual partnership in NATO. Furthermore, the big five English-speaking countries in the world, known as the Five Eyes, created a global intelligence network in 1946, underpinning this assumption. Although there is not much knowledge of the content of the agreement it can be assumed that they were heavily concerned about the post-WWII developments.[65]

Trust is very important for allies and friends. But instead of trusting that they will not spy on each other, they should instead trust that they are spying for the right reasons. That is to verify opposed to betray.[66] Being the political leader of Germany for over a decade and working nearly on a personal relation with President Obama for the last eight years, Chancellor Merkel was certainly personally offended by the NSA surveillance but most probably not politically surprised by the fact. Nevertheless, it is of utmost importance that states adhere to more restraining norms when "verifying" on allies in lieu of spying on adversaries. And with that said, it is time to propose some of these norms and other recommendations in regard to cyber-espionage.

64 SPIEGEL ONLINE, Hamburg, "Thatcher Und Die Wiedervereinigung: Eisernes Misstrauen," *SPIEGEL ONLINE*, accessed December 10, 2016, http://www.spiegel.de/einestages/margaret-thatcher-und-die-wiedervereinigung-a-951099.html.

65 "The Five Eyes | Privacy International," accessed December 17, 2016, https://www.privacyinternational.org/node/51; Five Eyes nations: Australia, Britain, Canada, New Zealand, and the United States; Interestingly, those nations do not have a "no spy" agreement among each other.

66 Leif-Eric Easley, "Spying on Allies," 142–45.

Old Norms in New Skins

States have always crossed ethical norms or those imposed by international law whenever the survival of the nation has been at risk—in the physical as well as in the virtual world. Most countries have even institutionalized ways to plan and conduct covert operations outside these norms with agencies like the CIA, and the only way for states to justify these actions is by labeling them as anticipatory self-defense. The study of states' practices provides an understanding of how nations apply international law or when they simply refuse to accept it.[67] In terms of "state practice," cyber-espionage is still in its infancy. Therefore, it is important to adapt, translate, and agree to new norms in cyberspace. This paper offers a few proposals to do so.

International Forum and Agreements

There is a great fear that the code used to enable cyber-espionage might also facilitate an attack. Simultaneously, the advantages of cyber-espionage for each state are so high that no one really wants to ban virtual spying in general. As developed nations become more and more dependent on cyber, they correspondingly become more vulnerable to cyber-attacks. Therefore, Clarke suggests that the leading states should begin to regularly meet for "cyber-talks."[68] The UN GGE has already started this kind of talks and provides a platform for cyber-nations to formulate their thresholds. Among others, they agreed to restrain themselves from operations against critical infrastructure and banned EMCE.[69] President Obama further clarified the definition of critical infrastructure with executive order 13010 and underpinned the U.S. red line in this matter. Among the eight categories are telecommunication nodes, electrical power

67 Ian Hurd, "The International Rule of Law: Law and the Limits of Politics."
68 Clarke and Knake, *Cyber War*, 268–69.
69 "2015 UN GGE Report."

systems, transportation systems, and the banking and finance sector.[70] This newly defined red line will certainly not prevent all cyber-espionage operations but it will definitely increase the inhibition threshold since crossing the line will cause repercussions and change the cost-benefit analysis in favor of the defender. Additionally, these measures can be further supported by other existing international institutions. For example, in the pursuit of nuclear energy states could grant unrestricted access to the International Atomic Energy Agency (IAEA), if there are any doubts about its peaceful purpose. As a trust building measure, this behavior would contribute to international stability and would prevent the need for cyber-espionage outside the rules. In a second step, the agreed norms have to be incorporated in future (non-cyber) agreements to gain more strength. The Trans-Pacific Partnership (TPP) trade agreement can serve here as a good example. The theft of IP is a serious threat to the economy of a state and has been incorporated into the TPP. A whole chapter of about seventy-five pages is devoted to this offense.[71] This treaty ensures that IP theft is not tolerated and opens more robust ways to respond to EMCE. But beside these international agreements, there are also norms which should states impose to themselves.

Ethical Considerations

The moral aspects when it comes to the challenge of trust among allies are more difficult to evaluate and twofold in nature. First, the spying country has to walk a fine line between sufficient insight to verify and too much interest that could be perceived as betrayal. Easley explains that France and Germany were disappointed because they are left out of the 'Five Eyes' intelligence agreement. Paris and Berlin complained that this is a "breach of trust", however,

70 Sharp, *Cyberspace and the Use of Force*, 22–23.

71 "The Trans-Pacific Partnership @ USTR.gov," *The Trans-Pacific Partnership @ USTR.gov*, accessed November 28, 2016, http://www.ustr.gov/tpp.

they did not feel betrayed.[72] Even though the "Five Eyes" nations did not conceal their agreement it caused resentments in Europe. To walk the line during cyber-espionage, however, will be even more difficult, especially since the interpretation between verify and betrayal depends on the perception of the offended state. The bottom line is that states should keep their monitoring activities among allies to the absolute minimum to serve their verifying needs and remain highly professional during the conduct. A closer look into the political activities should be expected but personal conversations or an indistinct interception of "whatever they can get" is definitely out of bounds. Unfortunately, the NSA Committee of Inquiry did not release the details of the alleged phone tapping of Chancellor Merkel's mobile phone by the NSA. However, the investigation on this special issue was closed by the Attorney General in 2015 due to lack of evidence.[73] It suggests that the United States was able to walk this line. The second aspect of the moral implications is in the hands of the attacked state. Nations should be aware that nothing is safe in cyberspace. Therefore, they should act honestly and professionally behind the scenes and restrain themselves from personal assaults or humiliating attitudes when communicating with each other. It is only a question of time until there will be another diclosure on the same scale as Snowden's, and talking badly behind someone's back can cause severe damage to international relations as well as to domestic politics.

72 Leif-Eric Easley, "Spying on Allies," 145.

73 "NSA-Affäre: Ermittlungen Zu Merkels Handy Eingestellt," *Die Zeit*, June 12, 2015, sec. Politik, http://www.zeit.de/politik/deutschland/2015-06/nsa-affaere-handy-ueberwachung-angela-merkel-ermittlungen-eingestellt.

Conclusion

International norms have always been contested from a legal or ethical perspective. Also, covert operations in general and espionage, in particular, have always been ambiguous and are not a new phenomenon in cyberspace. The reasons for deviating from norms in cyberspace will not be found in this specific domain but within the overarching context of international relation regardless of whether these relations are based on mutual trust or long lasting hostilities and mistrust. Perceived threats and a nation's intent are the intangibles that might legitimize crossing the norms or justify cyber-espionage from an ethical perspective. However, it is hardly possible to prove one or the other. The benefits of cyber-espionage outweigh the cost that might be caused by its ambiguity. Nevertheless, since ambiguity cannot be avoided in the cyber-domain, neither in intent (attack versus espionage), nor content (security versus EMCE), nor its ethical motive (trust versus betrayal), limits have to be articulated and agreed upon. Furthermore, the international community has to interweave these agreements into other mechanisms outside the virtual world to underpin their value and guarantee a robust response if violated. Lastly, it is of utmost importance that allies adopt very high and controlled ethical standards within their verifying policy to avoid damage to the unity of allies and their common values.

Bibliography

"2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law." *CCDCOE*, August 31, 2015. https://www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.

Brantly, Aaron F. "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace." *Intelligence and National Security* 31, no. 5 (July 28, 2016): 674–85. doi:10.1080/02684527.2015.1077620.

Center, Jewish Policy. "The Attack on Syria's Al-Kibar Nuclear Facility." *Jewish Policy Center*, February 28, 2009. https://www.jewishpolicycenter.org/2009/02/28/the-attack-on-syrias-al-kibar-nuclear-facility/.

"Charter of the United Nations | United Nations." Accessed November 28, 2016. http://www.un.org/en/charter-united-nations/index.html.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco, 2010.

"Cyber-Attacke: Hacker Knacken Geheimes Jet-Projekt - SPIEGEL ONLINE." Accessed December 17, 2016. http://www.spiegel.de/netzwelt/tech/cyber-attacke-hacker-knacken-geheimes-jet-projekt-a-620208.html.

Dueck, Colin. *Reluctant Crusaders: Power.* Princeton University Press, 2008.

"F-35 Capabilities." *F-35 Lightning II*. Accessed December 18, 2016. https://www.f35.com/about/capabilities.

"GCHQ and NSA Targeted Private German Companies - SPIEGEL ONLINE." Accessed December 16, 2016. http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.

Houghton, David Patrick. *The Decision Point: Six Cases in U.S. Foreign Policy Decision Making*. New York: Oxford University Press, 2013.

Ian Hurd. "The International Rule of Law: Law and the Limits of Politics." *Ethics and International Affairs* 28, no. 1 (2014): 39–51.

J. R. Clapper. "Statement for the Record, 'Worldwide Threat Assessment of the US Intelligence Community' before the House Permanent Select Committee on Intelligence." Edited by DNI, February 25, 2016.

Leif-Eric Easley. "Spying on Allies." *Survival* 56, no. 4 (September 2014): 141–56.

Libicki, Martin C. *Cyberspace in Peace and War*. Annapolis, Maryland: Naval Institute Press, 2016.

"Nato Review." Accessed December 4, 2016. http://www.nato.int/docu/review/2002/issue4/english/art4.html.

"NSA-Affäre: Ermittlungen Zu Merkels Handy Eingestellt." *Die Zeit*. June 12, 2015, sec. Politik. http://www.zeit.de/politik/deutschland/2015-06/nsa-affaere-handy-ueberwachung-angela-merkel-ermittlungen-eingestellt.

Office of General Counsil Department of Defense. “Department of Defense Law Manual,” June 2015.

“Operation Opera - Raid on Iraqi Nuclear Reactor | Jewish Virtual Library.” Accessed November 15, 2016. http://www.jewishvirtuallibrary.org/jsource/History/Osirak.html.

Owens, William A., Kenneth W. Dam, Herbert Lin, National Research Council (U.S.), National Research Council (U.S.), and National Research Council (U.S.), eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.

Parks, W. Hays. “The International Law of Intelligence Collection.” In *National Security Law*, edited by John Norton Moore, Frederick S. Tipson, and Robert F. Turner. Durham, N.C: Carolina Academic Press, 1990.

Radsan, A. John. “The Unresolved Equation of Espionage and International Law.” *Michigan Journal of International Law* 28, no. 3 (2007): 595–623.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. The Changing Face of War. Santa Barbara, Calif: Praeger, 2013.

Schmitt, Michael N., and NATO Cooperative Cyber Defence Centre of Excellence, eds. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York: Cambridge University Press, 2013.

Sharp, Walter Gary. *Cyberspace and the Use of Force*. Falls Church, Va: Aegis Research Corp, 1999.

Shattan, Joseph. *Architects of Victory: Six Heroes of the Cold War*. Washington, DC: Heritage Foundation, 1999.

“Snowden Archive.” *CJFE | Canadian Journalists for Free Expression*. Accessed December 16, 2016. http://www.cjfe.org/snowden.

SPIEGEL ONLINE, Hamburg. “Thatcher Und Die Wiedervereinigung: Eisernes Misstrauen.” *SPIEGEL ONLINE*. Accessed December 10, 2016. http://www.spiegel.de/einestages/margaret-thatcher-und-die-wiedervereinigung-a-951099.html.

“The Five Eyes | Privacy International.” Accessed December 17, 2016. https://www.privacyinternational.org/node/51.

“The Trans-Pacific Partnership @ USTR.gov.” *The Trans-Pacific Partnership @ USTR.gov*. Accessed November 28, 2016. http://www.ustr.gov/tpp.

Thomas Rid. “Cyber War Will Not Take Place.” *The Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32.

(ZDF), Zweites Deutsches Fernsehen. “US-Präsident in Berlin: Merkel Und Obama Werben Für TTIP - Heute-Nachrichten.” Accessed December 9, 2016. http://www.heute.de/treffen-im-kanzleramt-merkel-empfaengt-obama-und-wird-vom-us-praesidenten-gelobt-45923046.html.